IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): In an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network[[;]], [[an]] the address based authentication system ~~in which~~ including:

the authentication server which comprises

authentication means for authenticating a user based on the user authentication information transmitted as an authentication request from the user terminal;

an address allocating means for allocating an address to the user terminal for a successful authentication of the user;

~~authentication information~~ generating means for generating ~~information for authentication from information including~~ information-for-authentication using at least the allocated address;

a ticket issuing means for issuing a ticket containing the allocated address ~~allocated by the address allocating means~~ and the ~~information for authentication~~ information-for-authentication;

and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;

the user terminal which comprises

~~a user authentication information~~ transmitting means for transmitting the user authentication information to the authentication server for purpose of an authentication request;

a ticket reception means for receiving the ticket containing the allocated address transmitted from the authentication server;

means for setting up the allocated address contained in the ticket as a source address for [[a]] each packet which is to be transmitted from the user terminal to the application server;

means for transmitting a first packet including the ticket to the application server for establishing a session; and

a service request means for transmitting a second packet requesting [[a]] the service to the application server through the session;

and the application server which comprises

a ticket memory means for storing the ticket transmitted from the user terminal;

ticket verifying means for verifying the presence or absence of any forgery in the ~~information for authentication~~ information-for-authentication in the ticket transmitted from the user terminal and storing the ticket in the ticket memory means in the absence of a forgery;

an address comparison means for determining whether or not the allocated address contained in the ticket which is stored in the ticket memory means coincides with the source address of the ~~service request~~ second packet which is transmitted from the user terminal through the session; and

a service providing means for transmitting to the user terminal packets which ~~provides~~ provide [[a]] the service to the user when a coincidence between the addresses is determined by the address comparison means.

Claim 2 (Currently Amended): [[An]] The authentication system according to Claim 1

in which the user terminal has a key information ~~relating to~~ representing a public key of the user terminal,

the ~~user authentication information~~ transmitting means being ~~means for transmitting~~ configured to transmit the key information also together with the user authentication information, and the ticket issuing means being ~~means for issuing~~ configured to issue the ticket also containing the key information which is transmitted from the user terminal,

the user terminal further comprising

a first session key generating means for calculating a first session secret key which is shared with the application server, from a private key K_{SU} of the user terminal and a public key K_{PS} of the application server;

and a packet cryptographic processing means for ~~performing a~~ processing ~~upon a~~ each packet to be transmitted to the application server by the first session secret key to guarantee that there is no forgery in ~~the~~ each packet;

the application server further comprising

a second session key generating means for calculating a second session secret key which is shared with the user terminal, from a private key K_{SS} of the application server and a public key K_{PU} of the user terminal;

a packet verifying means for confirming whether or not ~~the~~ each packet received from the user terminal is forged using the second session secret key;

and wherein said ticket verifying means is configured to verify whether or not the key information contained in the ticket [[of]] in the first packet, which has been verified as not being forged, is the key information ~~relating to~~ representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means.

Claim 3 (Currently Amended): [[An]] The authentication system according to Claim 2

the application server further comprising

an address collating means for collating the allocated address in the ticket transmitted from the user terminal against the source address of the first packet which includes the ticket and for preventing the ticket from being stored in the ticket memory means if a coincidence is not found.

Claim 4 (Currently Amended): [[An]] The authentication system according to Claim 2 in which the authentication server comprises a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request for a successful authentication of the user,

the ticket issuing means being configured to issue ~~means for issuing~~ the ticket inclusive of the user identifier.

Claim 5 (Currently Amended): [[An]] The authentication system according Claim 1

in which the authentication information generating means of the authentication server is configured to process the information including the allocated address with a shared secret key which is shared beforehand between the authentication server and the application server,

the ticket verifying means of the application server is configured to further verify the ~~information for authentication~~ information-for-authentication contained in the ticket using a shared secret key which is beforehand shared between the authentication server and the application server.

Claim 6 (Currently Amended): [[An]] The authentication system according to Claim 1, wherein

the application server comprises an address collating means for collating the allocated address in the ticket which is transmitted from the user terminal against the source address of the first packet which includes the ticket and for preventing the ticket from being stored when a coincidence is not found.

Claim 7 (Currently Amended): An authentication server in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication[[;]], comprising

a ~~user authentication information~~ reception means for receiving an authentication request inclusive of a user authentication information and key information ~~relating to~~ representing a public key K_{PU} of the user terminal both transmitted from the user terminal;

an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication;

an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user;

authentication information generating means for generating ~~information for authentication from information including~~ information-for-authentication using at least the allocated address and the key information;

a ticket issuing means for issuing a ticket containing the allocated address ~~allocated by the address allocating means~~, the key information and the ~~information for authentication~~

information-for-authentication to the user terminal the user of which ~~whose user~~ is authenticated by the authentication means; and

a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal.

Claim 8 (Currently Amended): [[An]] The authentication server according to Claim 7, wherein the authentication information generating means is configured to generate the ~~information for authentication~~ information-for-authentication by processing ~~the information including~~ at least the allocated address and the [[ket]] key information using a shared secret key which is beforehand shared between the authentication server and the application server.

Claim 9 (Currently Amended): [[An]] The authentication server according to Claim 7, further comprising

a user identifier allocating means for allocating a user identifier which corresponds to the authenticated user in response to the authentication request when authentication of the user is successful,

wherein the authentication information generating means is configured to process the information including the allocated address, the key information and the user identifier to produce the ~~information for authentication~~ information-for-authentication and the ticket issuing means is configured to combine at least the ~~information for authentication~~ information-for-authentication, the allocated address, the key information and the user identifier to form the ticket.

Claim 10 (Currently Amended): [[An]] The authentication server according to Claim 9 in which the user identifier allocating means is configured to encrypt user information

which directly identifies the user by using an ~~identifier generating~~ identifier-generating secret key K_{ID} of the authentication server to produce the user identifier.

Claim 11 (Cancelled).

Claim 12 (Currently Amended): A user terminal in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, comprising

a ticket reception means for receiving a ticket transmitted from the authentication server, said ticket containing an address allocated to the user terminal, key information ~~relating to~~ representing a public key K_{PU} of the user terminal and ~~information for authentication~~ information-for-authentication produced by using at least ~~processing information including~~ the allocated address and the key information;

a source address set-up means to which the received ticket is input and which sets up the allocated address contained in the ticket as a source address of each packet to be transmitted to the application server ~~the user terminal~~;

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server;

a service request means for transmitting a second packet representing a service request to the application server through the established session;

a ~~key information~~ generating means to which [[a]] the public key K_{PU} of the user terminal is input and which generates [[a]] the key information ~~relating to~~ representing the public key K_{PU} of the user terminal;

a session key generating means to which a private key K_{SU} of the user terminal and [[an]] a public key K_{PS} of an application server are input and which calculates a session secret key which is shared with the application server;

[[and]] a packet cryptographic processing means to which [[a]] each packet to be transmitted from the user terminal and the session secret key are input and which ~~applies a processing to the transmitted~~ processes the packet using the session secret key to guarantee ~~which guarantees~~ that there is no forgery in ~~the~~ each packet ~~by the session secret key~~;

a user authentication information transmitting means configured to transmit the key information together with the user authentication information to the authentication server.

Claim 13 (Cancelled).

Claim 14 (Currently Amended): A user terminal ~~according to Claim 12, further comprising~~ in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, comprising:

a ticket reception means for receiving a ticket transmitted from the authentication server, said ticket containing an address allocated to the user terminal, key information representing a public key K_{PU} of the user terminal and information-for-authentication produced by using at least the allocated address and the key information;

a source address set-up means to which the received ticket is input and which sets up the allocated address contained in the ticket as a source address of each packet to be transmitted to the application server;

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server;

a service request means for transmitting a second packet representing a service request to the application server through the established session;

a key information generating means to which an authentication purpose shared secret key K_{US} which is shared with the application server and a random number ~~session dependent information~~ which changes each time a session is established are input and which generates a key information by processing the random number ~~session dependent information~~ by the authentication purpose shared secret key;

a session key generating means to which a private key K_{SU} of the user terminal and a public key K_{PS} of an application server are input and which calculates a session secret key which is shared with the application server;

a packet cryptographic processing means to which each packet to be transmitted from the user terminal and the session secret key are input and which processes each packet using the session secret key to guarantee that there is no forgery in each packet; and

a [[the]] user authentication information transmitting means ~~being means to~~ which is configured to transmit ~~the key information is also input and which transmits~~ the key information together with the user authentication information.

Claim 15 (Currently Amended): An application server in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication[[;]], comprising

a session establishing means for establishing a session with a user terminal in response to a reception of a session establishment request packet containing a ticket from the user terminal;

a ticket memory means in which [[a]] the ticket transmitted from the user terminal is stored;

an address comparison means to which a source address of a service request packet which is transmitted from the user terminal and received through the established session is input and which determines whether or not the source address coincides with [[the]] an allocated address of the user terminal contained in the ticket stored in the ticket memory means; and

a service providing means which ~~transmits packets for providing~~ provides a service to the ~~user to the~~ user terminal when the output of the address comparison means indicates a coincidence[[;]],

wherein said session establishing means comprises a ticket verifying means for verifying authenticity of the ticket, which is received ~~through a packet~~ from the user terminal for establishing the session, by checking the ~~information for authentication~~ information-for-authentication contained in the ticket and preventing the ticket from being stored in the ticket memory means when verification is not successful.

Claim 16 (Cancelled).

Claim 17 (Currently Amended): [[An]] The application server according to Claim 15, further comprising

a session key generating means for calculating a session secret key which is shared with the user terminal from a private key of the application server and [[an]] a public key of the user terminal;

and a packet verifying means for verifying whether or not [[a]] the session establishment request packet received from the user terminal is forged using the session secret key and for preventing the ticket from being stored in response to a verification output indicating the presence of a forgery.

Claim 18 (Currently Amended): [[An]] The application server according to Claim 17 in which the ticket verifying means comprises collating means for verifying, when the received session establishment request packet ~~which~~ has been verified by the packet verifying means as not forged, whether or not key information contained in the ticket corresponds to the public key of the user terminal which has been used in the calculation of the session secret key.

Claim 19 (Currently Amended): [[An]] The application server according to Claim 15 in which the ticket verifying means comprises terminal authenticating means to which an authentication purpose shared secret key which is shared with the user terminal and a random number ~~session dependent information~~ which changes each time a session is established are input and which processes the random number ~~session dependent information~~ using the authentication purpose shared secret key, collates a result of the processing against [[the]] a key information in the ticket and verifies the authenticity of the ticket by seeing whether or not a matching between the result of processing and the key information applies.

Claim 20 (Currently Amended): An application server according to Claim 15 in which the ticket verifying means comprises means for verifying whether or not the source address of the received session establishment request packet coincides with the allocated address contained in the ticket within the session establishment request packet and for preventing the ticket from being stored in response to a detection output which indicates a non-coincidence.

Claim 21 (Currently Amended): A computer readable storage medium having stored thereon an authentication server program for ~~allowing~~ programming a computer to function as an authentication server ~~as defined in Claim 7~~ in an authentication system in which an authentication of a user utilizing a user terminal is performed through the user terminal by an authentication server and a request is made to an application server to provide a service on the basis of the authentication, the authentication server comprising:

a user authentication information reception means for receiving an authentication request inclusive of a user authentication information and key information representing a public key K_{PU} of the user terminal both transmitted from the user terminal;

an authentication means to which the user authentication information of the received authentication request is input and which authenticates the user on the basis of the user authentication information and providing a signal indicating a successful authentication upon a successful authentication;

an address allocating means for allocating an address to the user terminal in response to an input of the signal indicating a successful authentication of the user;

authentication information generating means for generating information-for-authentication using at least the allocated address and the key information;

a ticket issuing means for issuing a ticket containing the allocated address, the key information and the information-for-authentication to the user terminal the user of which is authenticated by the authentication means; and

a ticket transmitting means to which the ticket is input and which transmits the ticket to the user terminal.

Claim 22 (Currently Amended): A computer readable storage medium having stored thereon a user terminal program for ~~allowing~~ programming a computer to function as a user terminal ~~according to Claim 12~~ in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, the user terminal comprising:

a ticket reception means for receiving a ticket transmitted from the authentication server, said ticket containing an address allocated to the user terminal, key information representing a public key K_{PU} of the user terminal and information-for-authentication produced by using at least the allocated address and the key information;

a source address set-up means to which the received ticket is input and which sets up the allocated address contained in the ticket as a source address of the user terminal;

a session establishing means to which the ticket is input and which transmits a first packet including the ticket to the application server for establishing a session with the application server;

a service request means for transmitting a second packet representing a service request to the application server through the established session;

a key information generating means to which the public key K_{PU} of the user terminal is input and which generates the key information representing the public key K_{PU} of the user terminal;

a session key generating means to which a private key K_{SU} of the user terminal and a public key K_{PS} of an application server are input and which calculates a session secret key which is shared with the application server;

a packet cryptographic processing means to which each packet to be transmitted from the user terminal and the session secret key are input and which processes each packet using the session secret key to guarantee that there is no forgery in each packet;

a user authentication information transmitting means configured to transmit the key information together with the user authentication information to the authentication server.

Claim 23 (Currently Amended): A computer readable storage medium having stored thereon an application server program for ~~allowing~~ programming a computer to function as an application server ~~according to Claim 15~~ in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, the application server comprising:

a session establishing means for establishing a session with a user terminal in response to a reception of a session establishment request packet containing a ticket from the user terminal;

a ticket memory means in which the ticket transmitted from the user terminal is stored;

an address comparison means to which a source address of a service request packet which is transmitted from the user terminal and received through the established session is

input and which determines whether or not the source address coincides with an allocated address of the user terminal contained in the ticket stored in the ticket memory means; and

a service providing means which provides a service to the user terminal when the output of the address comparison means indicates a coincidence,

wherein said session establishing means comprises a ticket verifying means for verifying authenticity of the ticket, which is received from the user terminal for establishing the session, by checking the information-for-authentication contained in the ticket and preventing the ticket from being stored in the ticket memory means when verification is not successful.

Claim 24 (Currently Amended): The system according to Claim 1, in which the authentication server has a secret key and a public key for a digital signature, ~~the step of generating the information for authentication at the authentication server is a step for computing a digital signature on the information including the allocated address using the secret key for the digital signature,~~

~~the ticket verifying step at the application server is a step for verifying the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server~~ and said ticket issuing means comprises:

an authentication information generating means for computing a digital signature on the information including at least the allocated address using the secret key for the digital signature to produce the information for authentication so that the application server can verify the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server.

Claim 25 (Currently Amended): The authentication server according to Claim 7, wherein the authentication server has a secret key and a public key for a digital signature, and said ticket issuing means comprises:

an authentication information generating means for computing a digital signature on the information including at least the allocated address using the secret key ~~for the digital signature~~ to produce the information for authentication so that the application server can verify the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server.